(12) UK Patent Application (19) GB (11) 2 202 981 (13) A

(43) Application published 5 Oct 1988

(21) Application No 8807742

(22) Date of filing 31 Mar 1988

(30) Priority data
(31) 8707672 (32) 31 Mar 1987 (33) GB

(71) Applicant
Satellite Video Systems Ltd

(Incorporated in United Kingdom)

2 Eastwood Avenue, Sandringham Park, Blyth, Northumberland, NE24 3RN

(72) Inventors
Dr Brian John Stanier
Harold Dodd

(74) Agent and/or Address for Service
Urquhart-Dykes & Lord
Midsummer House, 419B Midsummer Boulevard
Central Milton Keynes, MK9 3BN

(51) INT CL⁴
H04B 1/59

(52) Domestic classification (Edition J):
G4H 13D 14A 14B 14D 14G 60 NNA TG
U1S 1287 1288 1819 G4H

(56) Documents cited
None

(58) Field of search
G4H
Selected US specifications from IPC sub-class H04B

(54) Access control equipment

(57) Access control equipment comprises an interrogation unit (IU) having means (14) for emitting an interrogation signal, and a plurality of transponders (e.g. T), each transponder having a unique stored multi-bit identity code. The interrogation signal simultaneously interrogates these bits of all transponders within range in a serial manner. A group reply signal is sent back to the interrogation unit from any transponder having, in the bit being interrogated, a bit value matching that required by the interrogation signal. The interrogation unit is arranged to determine, from the series of received reply signals, the identity of each and every valid transponder within range.

The reply signals may differ in successive interrogation cycles, being encrypted according to a control code sent by the interrogation unit at the beginning of each cycle. The final reply in the cycle may depend on a further hidden identity code also.

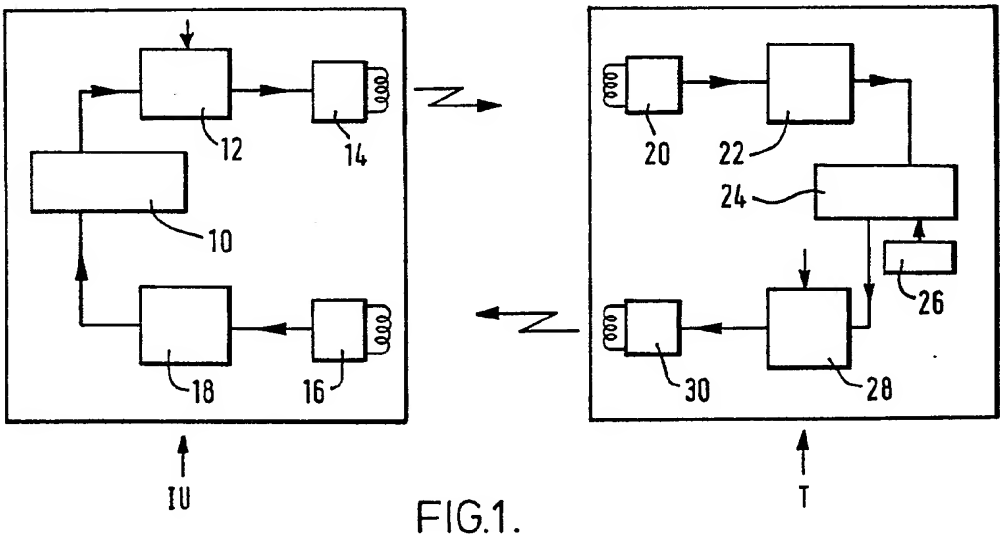

FIG.1.

GB 2 202 981 A

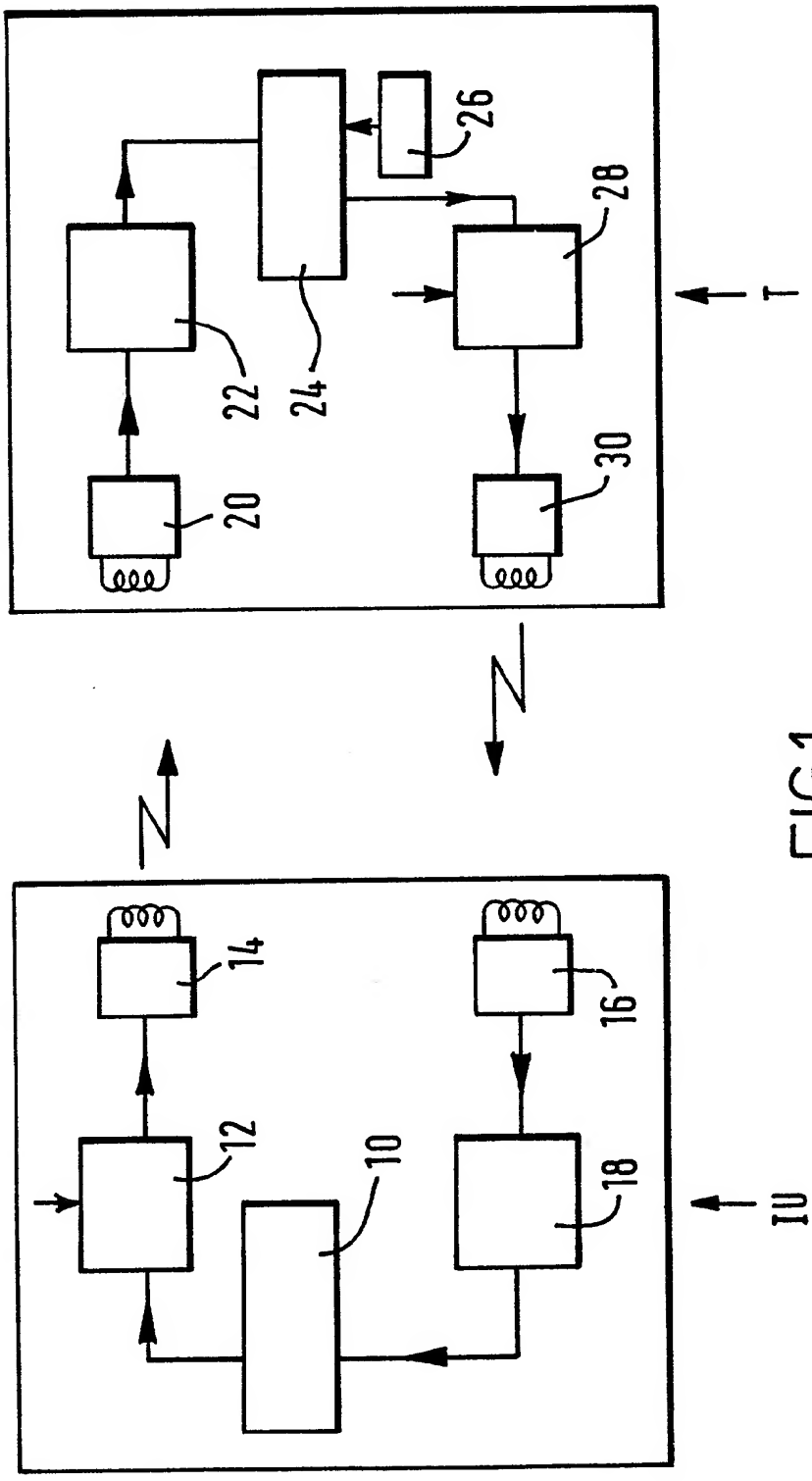

FIG.1.

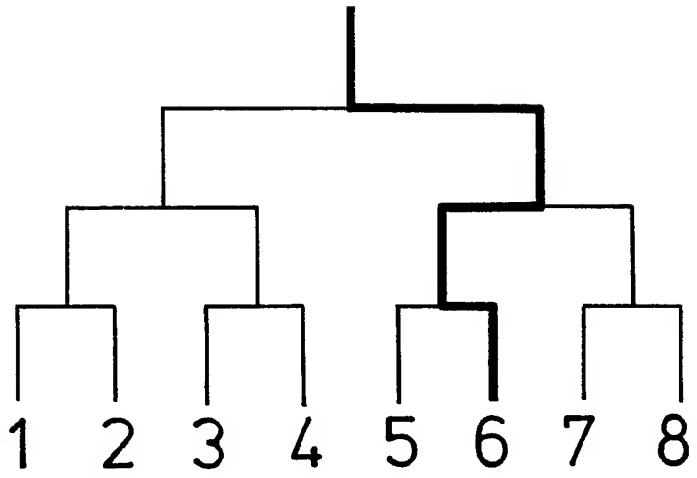

FIG.2.

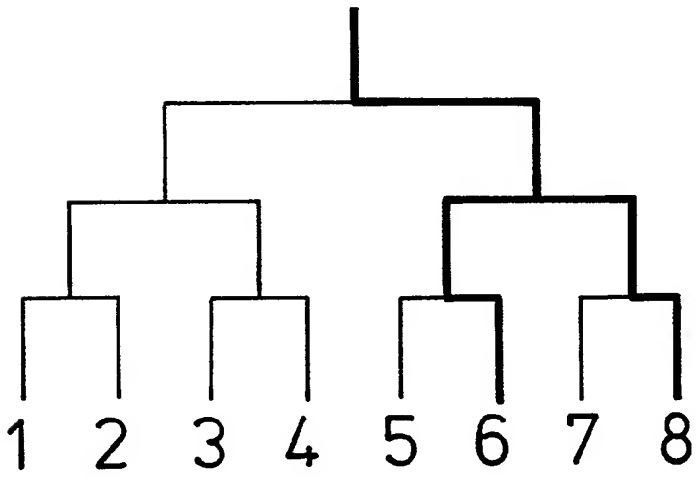

FIG.3.

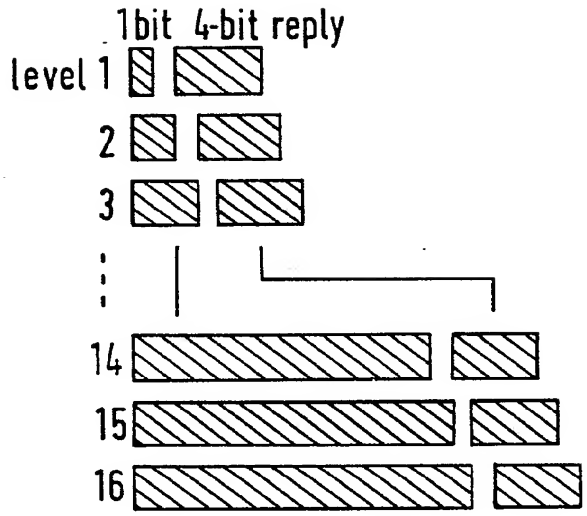

FIG.4.

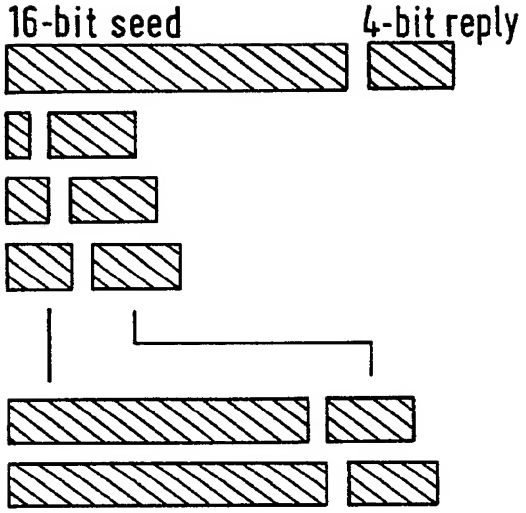

FIG.5.

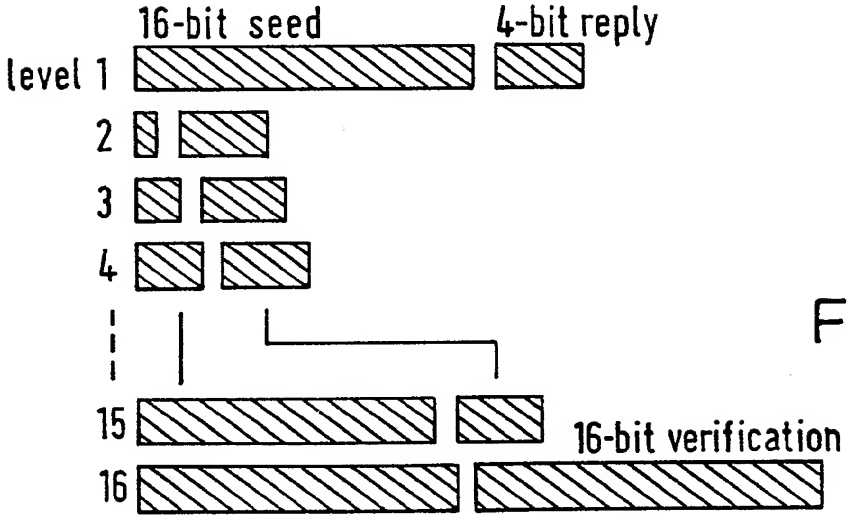

FIG.6.

ACCESS CONTROL EQUIPMENT

The present invention concerns access control equipment, that is electronic equipment designed to restrict unauthorised access to stored or transmitted data or to secure premises.

The control of such access is frequently afforded by the use of an interrogation unit and a transponder. At its simplest, the interrogation unit transmits an enquiry signal which may be received by any transponder within its range. The transponder is designed to modify the received signal in a predetermined manner and then retransmits the modified signal for reception by the interrogation unit. The modifying of the signal may be such as simply to distinguish between any "authorised" transponder and an unauthorised one or may be characteristic of the specific transponder alone, in which latter case the modified signal received by the interrogation unit identifies that transponder and no other.

Thus, if the transponder is carried by a person, vehicle, animal or piece of equipment then the interrogation unit is enabled to permit or reject access of a specific person or vehicle to controlled premises or to control access of a person or equipment to stored data. For example, when the equipment is capable of receiving transmitted data, it may be permitted to do so only when it has been identified or authorised by a correctly-

responding transponder.

Many systems of operating such equipment are known. For example, the interrogation unit may permanently or at intervals create a signal or field that will cause any transponder within range to identify itself. In a second system, any transponder coming within range will be caused to transmit an identifying signal to the interrogation unit. In a further alternative a transmission is initiated from the transponder and the interrogation unit processes the information so conveyed.

In such systems there is generally no problem in making a positive identification of a particular transponder, so long as that transponder is the only one within range of the interrogation unit, or the only one signalling the interrogation unit at a given time. Unless one of these criteria is met, then there can be difficulties in resolving the signals from the responders.

A further difficulty arises when the system protocol is such as to cause a transponder to transmit its same identifying signal more than once when traversing any interrogation field. Under these circumstances, the signal could be monitored by an unauthorised person, and thereafter reproduced in order to gain illicit access.

The present invention seeks to avoid these difficulties.

In accordance with this invention, there is provided access control equipment comprising an interrogation unit having means for emitting an interrogation signal, and a plurality of transponders having means for receiving the interrogation signal, each transponder having a stored identity code different from that of the other transponders, the identity code comprising a plurality of fields each holding an information bit selected from a plurality of possible bits, means for controlling the interrogation signal so that it simultaneously interrogates the fields of all transponders within range in a serial manner, means

for sending a group reply signal to the interrogation unit from any transponder having in the field being interrogated a bit matching that required by the interrogation signal, and means in the interrogation unit for converting the series of group reply signals to the encrypted identification codes of those transponders within range.

It will be seen that the equipment can operate irrespective of the number of transponders within range. The interrogation unit will analyse the series of group reply signals and will be informed by those signals of the identity codes of those transponders present. The responses are thus unable to interfere, and there is clear resolution of the signals. Furthermore, it will be appreciated that a transponder only transmits an identity code once in one whole interrogation sequence. Further interrogation requires a different identity code from the same transponder thus rendering it extremely difficult for an unauthorised person successfully to monitor and decipher that code. During most of the sequence each transponder simply sends a group reply signal.

Preferably each identity code is a binary word, each field comprising one bit, either 0 or 1. Other codes could be used, but binary is clearly the simplest. The interrogation and response sequence is preferably computer controlled, both in the interrogation unit and in the transponder, and binary identity logic obviously simplifies such control.

All responders sending a group reply signal in response to interrogation of a particular field will do so simultaneously, desirably with an identical signal. It would be possible to have the responders reply serially, each with a different signal falling within a group but this is not as rapid a method as simultaneous reply.

When binary logic is used, the transponders are effectively divided into classes and sets, and the

interrogation is effectively a binary tree search.

An embodiment of this invention will now be described by way of example only and with reference to the accompanying drawings, in which:

FIGURE 1 is a diagrammatic block diagram of access control equipment, showing an interrogation unit and one of a plurality of transponders of the equipment;

FIGURE 2 is a diagram to illustrate a tree search form of the interrogation process where only one transponder is present in the field of the interrogation unit;

FIGURE 3 is a similar diagram to illustrate the tree search when two transponders are present;

FIGURE 4 is a diagram to illustrate the data exchange for a 16-bit identifying code of the transponder;

FIGURE 5 is a similar diagram to illustrate the data exchange when a new 16-bit seed is transmitted on each search; and

FIGURE 6 is a similar diagram but where the transponder is arranged to return a hidden transponder code at the end of the search.

Referring to Figure 1, there is shown an access control equipment comprising an interrogation unit IU and a plurality of transponders, which may be in the form of tags, one only being shown at T. The interrogation unit IU comprises a microprocessor 10 one function of which is to generate interrogation signals and apply these to a pulse length modulator 12, which applies the modulated signals to a transmitter 14. The transmitter includes a coil for inductively coupling with a coil of a receiver 20 of the transponder or tag T. Receiver 20 of the transponder applies its received signal to a demodulator 22, the demodulated signal being applied to a microprocessor 24. This is able to refer to a memory 26 containing an identifying code of the transponder. The microprocessor 24 determines when a reply is to be made, in which case

it provides a reply signal to a phase shift modulator 28 driving a transmitter 30. A coil of this transmitter is inductively coupled with a coil of a receiver 16 of the interrogation unit and a demodulator 18 serves to recover the reply signal and pass this to the microprocessor 10 of the interrogation unit for decoding and identifying the transponder or transponders within range. The transmitting channel from the interrogation unit to the transponders may typically operate at 132 kHz and the reply channel may typically operate at 66 kHz.

The identifying code of each transponder may simply comprise a binary word. In use, the interrogation unit conducts a search by simultaneously interrogating the bits of all transponders within range in a serial manner. If any one or more transponders within range has a bit of predetermined value (e.g. 1) at the interrogated position in the binary word, that transponder (or those transponders) will transmit a reply simply to indicate this. Then the search proceeds by interrogating another position in the binary word to see if any transponder within range has a bit of predetermined value at that position, and so on. By decoding the reply signals received from this succession of interrogations, the microprocessor 10 in the interrogation unit can determine the identifying code of each transponder which is within range.

The interrogation process may take the form of a binary tree search. For example, in Figure 2 a single transponder with code 5 is assumed to be present. The identificiation commences by enquiring whether the transponder is a member of set (1,2,3,4) or set (5,6,7,8). The transponder responds to the latter and sends a first group reply signal. At level two of the search the choice is between (5,6) or (7,8) and (5,6) is identified whereupon a second group reply signal is sent. Finally, the transponder is recognised as (5) after the sending of a third

group reply signal and analysis by the interrogation unit. It may be convenient to regard the transponder identity as a binary number and each level of the search establishing 1 bit of the number. An n-bit number requires an n-level search and can identify 1 of 2^n transponders.

Only one interrogation is actually needed to establish to which set a single transponder belongs to each level. So n levels need n interrogations. Even for small n the search time is better than or equivalent to a simple polling of every single transponder identity code, but for higher values of n the saving becomes very large. For example, identification of 1 transponder from 65536 is possible with just 16 interrogations.

The simple search outlined above for a single transponder needs to be modified if multiple transponders are present. Every member of a set must respond to the IU when interrogated. This has three implications.

(a) If more than one member of a set is present all will respond. To avoid conflict they must either send identical replies simultaneously (so that the IU sees only one effective reply) or they may send different replies in sequence. The former is faster and does not require any timing or arbitration scheme.

(b) One or more transponders may be present in both sets at a tree level. It is then necessary to have two effective interrogations at each level instead of the single interrogation which was adequate for the single transponder case.

(c) The IU must remember when members of both sets at a given level are present and search both branches of the tree from that mode to identify all the transponders present. Figure 3 shows a possible search route for the case where both transponder 5 and transponder 8 are present.

The simplest (and fastest) tree search requires that the IU sends an interrogation data word whose length

is the minimum needed to identify the search level. At level 1 only 1 bit is needed. Level 2 needs 2 bits etc. The final level requires an n-bit word.

In principle the reply need only be a 1-bit word at any and every level. However it is preferable for the transponder to do some processing of the incoming data and a 4-bit reply is a suitable compromise between speed and complexity. Very little time can be allowed between receipt of the incoming data and the appropriate reply to avoid impeding the search and a simple pseudo-random sequence generation process yielding the 4-bit reply is an adequate compromise between speed and security at this stage. This form of data exchange is shown in Figure 4 for the example of a 16-bit tag code.

For security it is desirable that the transponder replies differ on successive searches. A simple way of ensuring this is to provide a new seed for the pseudo-random sequence generation at the beginning of each search. The seed would be generated by the IU (and could itself be part of a pseudo-random sequence). Transmission of (say) a 16-bit seed can replace the 1st level interrogation. This word can also be used as a synchronising signal to the transponder(s) for the start of a search.

The search pattern then becomes as shown in Figure 5. Note that the interrogation words for levels 2-16 can be reduced by 1 bit.

The transponder identity code revealed by the tree search is not in itself secure. It (or something equivalent to it) could possibly be deduced from a study of the search pattern and the corresponding replies. The security at this stage comes from the correct electronic and numerical forms of the replies and their relation to the interrogation data as determined by the transponder processor program. This is effectively the group reply signals and the code may be termed the public transponder

identity code.

Further security is provided by a verification procedure in which a transponder replies to the final interrogation with a 16-bit reply (say) generated from the seed provided at the beginning of the search and an internally stored or hidden 16-bit code (say) and possibly from the public transponder identity code. According to the stored algorithm this can only occur at the last search level because only then can no more than one transponder reply at a time.

The hidden code is derived from the public transponder code and a system key or code by any suitable algorithm. The IU could then regenerate the proper hidden code (and the appropriate transponder identified by the search.

The use of a key in the latter method allows customising a transponder set to a particular installation. For example, if the key is a 16-bit number then the total effective transponder code becomes 32 bits i.e. 4×10^9 different transponder identities. (65536 transponders in each of 65536 installations).

Figure 6 shows the information exchange for a typical single transponder search including the initial seed transmission and the final hidden transponder identity verification. The total data transmission to the transponder in this example requires 136 bits and the replies need 152 bits in this case.

The public and hidden transponder identities are held in the memory 26 of each transponder and are programmable. At initial power-up during manufacture, the identity codes will be set to some known values.

Programming after manufacture, and at any subsequent time, may be accomplished by transmitting the new identity codes to a transponder using an extension of the data exchange protocol outlined above.

For security reasons the programming messages are only accepted by a transponder immediately following a successful search and verification procedure and must contain sufficient error detection to avoid false programming.

The transponders utilised in the invention are desirably encapsulated transponders as described in GB-A-2164825, but utilising either a microchip processor and memory or customised large scale integrated circuits instead of the logic elements shown in that document. Each transponder may or may not incorporate its own battery, but if a battery is incorporated the transponder is capable of switching from and to a standby, power conserving mode in response to the presence or absence of a signal from the interrogation unit.

It will be appreciated that in the equipment described, the interrogation unit uniquely identifies each and every valid transponder present within the range during one complete interrogation cycle. Preferably, as described above, the transponder reply signals differ on successive interrogation cycles and on successive search steps within each cycle, being encrypted according to a different control code (the seed) transmitted at the beginning of each cycle.

CLAIMS

1. Access control equipment comprising an interrogation unit having means for emitting an interrogation signal, and a plurality of transponders having means for receiving the interrogation signal, each transponder having a stored identity code different from that of the other transponders, the identity code comprising a plurality of fields each holding an information bit selected from a plurality of possible bits, means for controlling the interrogation signal so that it simultaneously interrogates the fields of all transponders within range in a serial manner, means for sending a group reply signal to the interrogation unit from any transponder having in the field been interrogated a bit matching that required by the interrogation signal, and means in the interrogation unit for converting the series of group reply signals to the encrypted identification codes of those transponders within range.

2. Access control equipment as claimed in claim 1, in which the transponder reply signals differ on and during successive searches and are encrypted according to a different control code transmitted by the interrogation unit at the beginning of each interrogation cycle.

3. Access control equipment as claimed in claim 2, in which a valid transponder within range of the interrogation unit replies to its final interrogation step with an encoded signal generated from the control code transmitted at the beginning of the interrogation cycle and from a further identification code and an algorithm both held by the transponder.

Published 1988 at The Patent Office, State House, 66/71 High Holborn, London WC1R 4TP. Further copies may be obtained from The Patent Office,